## Remarks

Claims 1-22 are pending in this application, of which claims 1 and 13 are independent. By this amendment, independent claims 1 and 13 are amended. No new matter has been added. Based on the above amendments and the following remarks, Applicants respectfully request reconsideration and allowance of the application.

## Current Status of Rejection – Inappropriate Final Rejection

Based on prior conversations with the Examiner formerly examining this application, Examiner Leynna Ha, and further conversations with Supervisory Examiner Kim Vu and current Examiner Beemnet Dada, Applicants respectfully submit that the final office action of July 13, 2007, should not have been a final office action, and should instead have been a non-final office action.

In particular, and as was presented by Applicants in the last response filed April 30, 2007, Applicants did not receive a copy of the non-final office action of October 31, 2006, until April 27, 2007, only three days immediately prior to the expiration of the statutory period for reply, April 30, 2007. According to Examiner Ha, the office action of October 31, 2006, was returned to the Office undelivered, and despite Applicants efforts to have the address of record changed, the Office neglected to send the office action to the proper address of record. Because of the failure of the Office to resend the office action to the correct address, Applicants did not have sufficient time to fully prepare a response, and were forced to prepare a response in only three days. Examiner Ha agreed that this burden was unreasonable, and assured Applicants that the next office action, if needed, would be a non-final office action.

However, Applicants understand that Examiner Ha had an unexpected leave from the Patent Office, and as such, this application was transferred to Examiner Dada for further Examination. Examiner Dada, who was apparently unaware of the status of this case and the assurances of Examiner Ha that the next office action would be a non-final office action, issued the currently outstanding Final Office Action on July 13, 2007.

In view of the current after-final status of this application, and to prevent further confusion, Applicants enclose herewith a transcription of a voicemail from Supervisory Examiner Kim Vu received since the outstanding final office action was mailed explaining the confusion with this case and recommending that Applicants submit a response to the outstanding office action and indicating that the next office action will be a non-final office action.

> Hi, this is Kim Vu from the U.S. Patent and Trademark Office returning your phone call. I'm sorry about this situation because Examiner Leynna, she went under emergency so some of her cases were transferred and of course she did not pass along what she promised you. But the way the Palm system created it can it leave it tricky that when we sent out a final, it cannot be resent as a non-final. *The only thing that can be done is that if you can respond to that final now, just send in a letter stating the fact like that, then it acted like a response on the final, then we can send out the Office Action as a non-final, and reset the time at the same time*. That's the best that they can do because it is the Palm system, the way that it is when you sent out something, their looking for something to come back. It's almost very hard for us to resend something with that, so if you don't mind just send a letter, it does not have to be 2, 3 pages long, just 1 page long and *explain the situation as it was and act as a response to what was sent to out to you and we can resend the office action as a non-final*. Alright so if you have any further questions you can call me back at 571-272-3859. Thank-you. (Voicemail from Supervisory Examiner Vu)

Based on the above statements by Supervisory Examiner Vu, Applicants respectfully request that Examiner Dada issue the next office action (if deemed necessary after consideration of the amendments and remarks presented herein) as a non-final office action to afford Applicants sufficient opportunity to handle the prosecution of this application in a complete and thorough manner. Of course, if further explanation is needed, Examiner Dada or Supervisory Examiner Vu is invited to contact the undersigned at any time.

**Rejections under 35 U.S.C. § 103(a)**

Claims 1-8, 10-20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,084,969 to Wright et al. and U.S. 6,587,946 to Jakobsson. In addition, claims 9 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and the article entitled Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition).

However, as was discussed with the Examiner during the interview on August 24, 2007, none of the applied references, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1-8, 10-20, and 22, as presented herein.

For example, independent claim 1 recites, in relevant part, a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document, encrypting the original document with the session key to create an encrypted document, generating a proxy key based on a public key corresponding to the selected recipient, wherein the proxy key may be published without compromising its security, and *wherein the proxy key is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process*, and applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, *wherein the transformation may occur in an untrusted environment without compromising its security*, and wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

In addition, independent claim 13 recites, in relevant part, a system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising a session key generation system that generates a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document, an encryption system that encrypts the original document with the

session key to create an encrypted document, a proxy key generation system that generates a proxy key based on a public key corresponding to the selected recipient, *wherein the proxy key may be published without compromising its security, and wherein the proxy key is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process*, and a transformation system that applies the proxy key to the encrypted document to transform the encrypted document into a transformed document, *wherein the transformation may occur in an untrusted environment without compromising its security*, and wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

Thus, claims 1 and 13 recite that the generated proxy key *may be published without compromising its security*, and that *the proxy key is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process*. Therefore, as is clear from the amended claims, a proxy key is a key that is used to transform a message encrypted for one recipient into a message encrypted for another recipient without decrypting the message in the process.

In addition, claims 1 and 13 recite that the transformation of the encrypted document into a transformed document *may occur in an untrusted environment without compromising its security* and that *the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation*. Thus, as is clear from the amended claims, the transformation may occur in an untrusted environment without compromising its security.

In support for these claimed features, the Examiner's attention is respectfully directed to page 23, lines 18-23, of the Specification which provides that the proxy keys "may be published without compromising its security" and that the proxy transformations may be "applied in untrusted environments." In contrast, in a private scheme, when a proxy key is transferred from the grantor to the facilitator and grantee, care must be taken to protect the

proxy key from disclosure. As a result, the proxy transformation which uses the proxy key must be performed in private as well. (See page 23, lines 18-23, of the specification).

At least these features are not disclosed, suggested, or rendered obvious by the teachings of the applied references, alone or in combination.

Instead, Wright merely discloses a way of using a proxy (server) to decrypt and re-encrypt a message. In particular, the Examiner asserts that Col. 10, lines 26-28, and Col. 11, lines 11 and 65-67, and col. 14, lines 35-36, of Wright disclose "generating a proxy key based on a public key corresponding to the selected recipient." Applicants respectfully submit that this is not correct.

In particular, Col. 10, lines 26-28, reads as follows: "The user identification number (UID) . . . is used to indicate the source of the message so as to enable the pager proxy to retrieve the appropriate public decryption key (pb.sender)." This portion of Wright refers to the sender's key not to a public key corresponding to the selected recipient, as is recited in claims 1 and 13. Moreover, there is no suggestion whatsoever in Wright to generate a proxy key, much less a proxy key that may be published without compromising its security or a proxy key that is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process, as is recited in claims 1 and 13.

Col. 11, line 11, of Wright disclose "information stored in memory, including private and public key of the pager." The public key of the pager, i.e. the recipient, is mentioned, but there is no discussion of generating a proxy key based thereupon, much less a proxy key having the other claims features.

Col. 11, lines 65-67, of Wright disclose "the pager proxy 7 includes a database of public keys corresponding to the unique public keys of pagers registered with the encryption service provider that operates the proxy server." Once again, the public key of the pager, i.e. the recipient, is mentioned, but there is no discussion of generating a proxy key based thereupon, much less a proxy key having the other claimed features.

Finally, Col. 14, lines 35-36, of Wright disclose "... field 2 of the packet is *decrypted* by the private key of the destination pager (step 410) and then by the public decryption key of the pager proxy server (step 420) based on the encryption method identified by the identifier in field 1." This quote refers to two decryption steps using the private key of the pager and the public decryption key of the server. It does not refer to the generation of a proxy key based upon the public key of the pager/recipient.

Moreover, there is no suggestion whatsoever in Wright that any sort of transformation occurs, or that any such transformation may occur in an untrusted environment without compromising its security, as is recited in the claims. Instead, the methods disclosed by Wright clearly use a traditional decryption / encryption method, which cannot be used in an untrusted environment without compromising its security.

Thus, for at least the above reasons, and as was presented to the Examiner during the interview, Wright fails to disclose, suggest, or render obvious the generation of a proxy key based upon the public key of the recipient. Moreover, even if the step of generating a proxy key is set aside, as an example, use of the pager's public key as a "proxy key" would result in a non-functional system wherein any recipient could convert encrypted messages for others into encrypted messages for themselves thereby rendering such a system completely non-secure. That is why a separate proxy key needs to be generated based upon the public key of the recipient.

Similarly, contrary to the Examiner's assertions otherwise, Jakobsson also fails to disclose or suggest claimed invention, including the generation of a proxy key based upon the public key of the recipient. Instead, Jakobsson disclosed the use of the sender's private key (split into a number of shares) by quorum of proxy servers to perform the proxy transformation. It does not, however, use the recipient's public key to generate a proxy key, much less a proxy key having the other claimed features.

Moreover, there is no suggestion whatsoever in Jakobsson that any sort of transformation occurs, or that any such transformation may occur in an untrusted environment without compromising its security, as is recited in the claims.

The Irish Times article completely fails to overcome the above-stated deficiencies of Wright and Jakobsson.

Therefore, for at least the above reasons, none of Wright, Jakobsson, or the Irish Times article, taken alone or in combination, disclose, suggest, or render obvious, the invention recited in claims 1-22 under 35 U.S.C. § 103(a). Therefore, Applicants respectfully request that the rejections of claims 1-22 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

The present amendment is submitted in accordance with the provisions of 37 C.F.R. §1.116, which after Final Rejection permits entry of amendments placing the claims in better form for consideration on appeal. As the present amendment is believed to overcome outstanding rejections under 35 U.S.C. § 103, the present amendment places the application in better form for consideration on appeal. It is therefore respectfully requested that 37 C.F.R. §1.116 be liberally construed, and that the present amendment be entered.

**Except** for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

**NIXON PEABODY, LLP**

Date: October 11, 2007

/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler

**Customer No.: 22204**
**NIXON PEABODY LLP**
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000